DOD PRIVACY IMPACT ASSESSMENT (PIA) FORMAT

1. Department of Defense Component:

U. S. Army, Assistant Chief of Staff for Installation Management (ACSIM), Family & Morale, Welfare and Recreation Command (F&M WRC)

2. Name of Information Technology (IT) System (APMS System Name)

General Libraries Information System (GLIS)

3. Budget System Identification Number (SNAP-IT Initiative Number).

9990 DoD Information Technology Portfolio Repository

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)).

DA8794

5. IT Investment (OMB Circular A-11) Unique Identifier (if applicable).

N/A

6. Privacy Act System of Records Notice Identifier (if applicable).

A0215-1 DAPE – Library Borrowers'/Users' Profile Files (August 3, 2005, 70 FR 44581)

7. OMB Information Collection Requirement Number (if applicable) and expiration date

N/A

8. Type of authority to collect information (statutory or otherwise).

5 U.S.C. 301, Departmental Regulations
E.O. 9397 (SSN),
10 U.S.C. 3013, Secretary of the Army;
Public Law 106-554, Children's Internet Protection Act;
AR 215-1, Morale, Welfare, and Recreation Activities and Nonappropriated Fund
    Instrumentalities;
AR 25-97, The Army Library Program.

9. Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries, and interconnections, location of system and components, and system backup).

This library system's purpose is to manage library property, to identify individuals authorized to borrow library materials; to ensure that all library property is returned and individuals' accounts are cleared; to provide the librarian useful information for selecting, ordering, and meeting user requirements; and to help end users find materials in the library or on the Internet. GLIS combines the business operations of a library and web based access for its customers. Lifecycle phase of the hardware is operations and support. The system owner is the Family and MWR Command, Library Program. It is maintained for use by active duty, retirees, civilians and family members. FMWRC pays for software and hardware annual maintenance. More than 58 libraries around the world currently use the GLIS system. The servers are hosted at Fort Belvoir, Virginia, with a back up server in Heidelberg Germany. It is accessed through Army Knowledge Online (AKO) and offers single sign-on to the web-based catalog. The system connects to the Defense Enrollment Eligibility Reporting System (DEERS) to authenticate and provide data on users. Each library has a Personal Computer (PC) Management module, which controls access, schedules use and limits printing. The PC Management module allows libraries to comply with the Children's Internet Protection Act. This module reports to a database hosted at AKO. Both servers, which replicate in near real time, are backed up to tape daily. The system synchronizes the Bluecoat filter, the PC Reservation Module and the user database to identify children under the age of seventeen, using their birth date, and block inappropriate web sites on library computers. GLIS staff determines the types of web sites to be blocked. Materials checked out to an individual are attached to the individual's record until the materials are returned to the library. If materials are not returned, overdue notices are sent by e-mail or regular mail, and the individual's record may be blocked if they do not return the materials after several notices.

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g., names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.).

Name, dependent name, Social Security Number (SSN), common access card information, work address, home address, work phone, home phone, rank, branch of service, date of birth, work e-mail, home e-mail, dependent relationship, name of sponsor, sponsor activation begin/end dates, region codes, employee ID or driver's license number, materials & publications checked out or reviewed by individuals. Electronic Data Interchange Personal Identifier (EDI_PI) and Sponsor Electronic Personal Identifier are collected.

11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.).

The data is entered into the database by staff keyboard entry from information provided either orally, through a web based form, a local paper form or an electronic connection to the database.

12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a DA program, etc.)

The information is collected to identify individuals authorized to borrow library materials; to ensure that all library property is returned and individual's account is cleared; to provide librarian useful information for selecting, ordering, and meeting user requirements; to comply with the Children's Internet Protection Act; to provide authentication for borrowed electronic resources (e.g., e-books, e-journals); and to assist the individual in verifying materials charged against their account, renewing materials and requesting materials.

13. Describe how the information in identifiable form will be used (e.g., to verify existing data, etc.).

Authorized library staff will browse data to verify the correct person is checking out material and that the addresses are current for overdue and other notices to the individual.

14. Describe whether the system derives or creates new data about individuals through aggregation.

This system does not create new data about individuals through aggregation

15. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies).

Information will be available to authorized users with a need to know in order to perform official government duties. Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include DOD IG, DCIS, Army Staff Principals in the chain of command, DAIG, AAA, USACIDC, INSCOM, PMG and ASA FM&C. In addition, the DoD blanket routine uses apply to this system. This system interfaces with the Defense Eligibly Enrollment System to authenticate library users.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.

The library staff provides a copy of the Privacy Act Advisory Statement when an individual registers to use the library the first time. If individuals do not want the SSN used, they can state that at the time of registration. Without the SSN, GLIS will not be able to update information in DEERS, so the individual may have limited use of the library materials. GLIS staff may request another identifying number such as an employee ID or driver's license number.

17. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.

The individual is provided a Privacy Act Statement upon registration.

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

Access to the data is on a need to know basis and is available only to staff who are authorized access to the military network. Accounts with passwords are role based. The System administrator at FMWRC assigns logins restricted by function. Library customers can see only their own data using the single sign-on through AKO.

Library staff logins are role based so that staff without need to know privacy information are restricted in what they can see. All staff members are trained not to misuse the personal information in the system. Libraries have privacy policies posted and explain the policy to new staff & new customers.

This system has a current certification and accreditation. The system resides on secure military installations within secured facilities.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program," November 11, 2004. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur.

Yes. A0215-1 DAPE: Library Borrowers'/Users' Profile Files, Date: August 3, 2005, Federal Register Number: 70 FR 44581.

20. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.

Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. There are no risks in providing individual the opportunity to object or consent.

Due to privacy concerns, records of books checked out to an individual are not kept after the books are returned. The government cannot access an individual's reading history.

To prevent asking for privacy information each time a person uses the library, after the person has registered, the library staff will check out materials using the bar code on their CAC card, Military family member ID, retiree or other ID.

21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.

The data in the system is For Official Use Only. The PIA may be published in full.